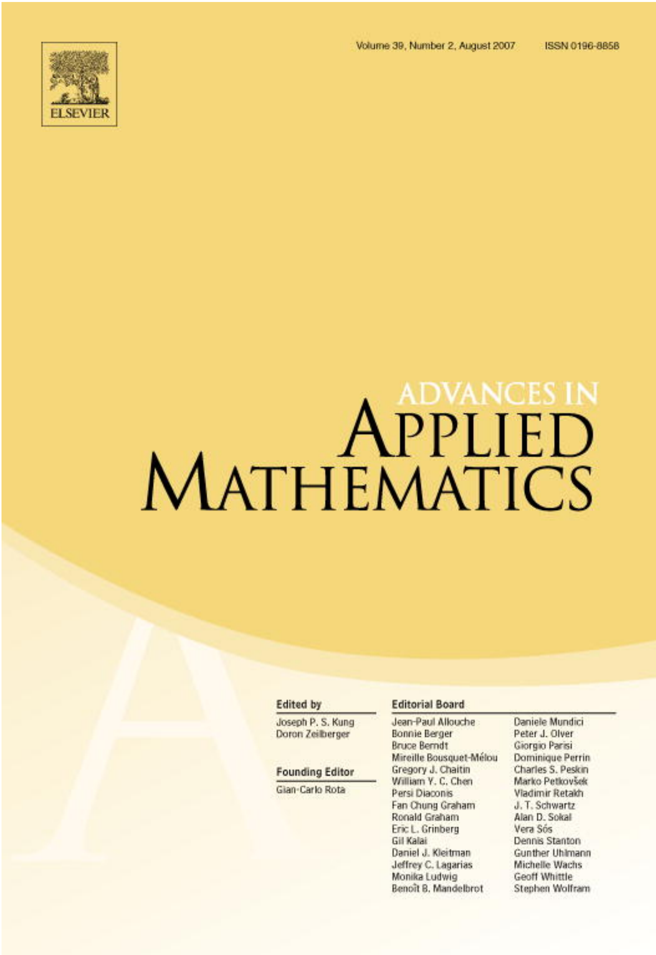
Volume 39, Number 2, August 2007
ISSN 0196-8858
ELSEVIER
ADVANCES IN
APPLIED
MATHEMATICS
Edited by
Joseph P. S. Kung
Doron Zeilberger
Founding Editor
Gian-Carlo Rota
Editorial Board
Jean-Paul Allouche
Bonnie Berger
Bruce Berndt
Mireille Bousquet-Mélou
Gregory J. Chaitin
William Y. C. Chen
Persi Diaconis
Fan Chung Graham
Ronald Graham
Eric L. Grinberg
Gil Kalai
Daniel J. Kleitman
Jeffrey C. Lagarias
Monika Ludwig
Benoît B. Mandelbrot
Daniele Mundici
Peter J. Olver
Giorgio Parisi
Dominique Perrin
Charles S. Peskin
Marko Petkovšek
Vladimir Retakh
J. T. Schwartz
Alan D. Sokal
Vera Sós
Dennis Stanton
Gunther Uhlmann
Michelle Wachs
Geoff Whittle
Stephen Wolfram

Available online at www.sciencedirect.com
ScienceDirect
Advances in Applied Mathematics 39 (2007) 269–281
ADVANCES IN Applied Mathematics
www.elsevier.com/locate/yaama

Counting permutations by congruence class of major index

Hélène Barcelo [a], Bruce E. Sagan [b,*], Sheila Sundaram [c]

[a] *Department of Mathematics, Arizona State University, Tempe, AZ 85287-1804, USA*
[b] *Department of Mathematics, Michigan State University, East Lansing, MI 48824-1027, USA*
[c] *Department of Mathematics, Bard College, Annandale-on-Hudson, NY 12504-5000, USA*

Received 29 December 2005; accepted 16 March 2006

Available online 8 June 2006

This paper is dedicated to the memory of Bob Maule who did seminal work on the subject

Abstract

Consider S_n, the symmetric group on n letters, and let $\operatorname{maj}\pi$ denote the major index of $\pi \in S_n$. Given positive integers k, l and nonnegative integers i, j, define

$$m_n^{k,l}(i,j) := \#\{\pi \in S_n\colon \operatorname{maj}\pi \equiv i \pmod{k} \text{ and } \operatorname{maj}\pi^{-1} \equiv j \pmod{l}\}.$$

We give a bijective proof of the following result which had been previously proven by algebraic methods: If k, l are relatively prime and at most n then

$$m_n^{k,l}(i,j) = \frac{n!}{kl}$$

which, surprisingly, does not depend on i and j. Equivalently, if $m_n^{k,l}(i,j)$ is interpreted as the (i,j)-entry of a matrix $m_n^{k,l}$, then this is a constant matrix under the stated conditions. This bijection is extended to show the more general result that, for $d \geqslant 1$ and k, l relatively prime, the matrix $m_n^{kd,ld}$ admits a block decomposition where each block is the matrix $m_n^{d,d}/(kl)$. We also give an explicit formula for $m_n^{n,n}$, and show that if p is prime then $m_{np}^{p,p}$ has a simple block decomposition. To prove these results, we use the representation theory of the symmetric group and certain restricted shuffles.

* Corresponding author.
E-mail addresses: barcelo@asu.edu (H. Barcelo), sagan@math.msu.edu (B.E. Sagan), sundaram@bard.edu (S. Sundaram).

0196-8858/$ – see front matter
doi:10.1016/j.aam.2006.03.002

MSC: 05A10; 05A19; 11B50

Keywords: Inversion; Major index; Permutation; Shuffle

1. Introduction

Let S_n denote the symmetric group consisting of all permutations π of the set $[n] := \{1, 2, \dots, n\}$. If we write $\pi = a_1 a_2 \dots a_n$ then the *major index of* π is

$$\operatorname{maj} \pi := \sum_{a_i > a_{i+1}} i.$$

Let k, l be positive integers and let i, j be nonnegative integers. We wish to study the cardinalities

$$m_n^{k,l}(i, j) = \#\{\pi \in S_n\colon \operatorname{maj} \pi \equiv i \pmod k \text{ and } \operatorname{maj} \pi^{-1} \equiv j \pmod l\}.$$

We will often omit the superscript k, l both for readability and because the parameters will be clear from context. Note that directly from the definition we have $m_n^{k,l}(i, j) = m_n^{l,k}(j, i)$. One of our main objectives is to give a bijective proof of the following theorem.

Theorem 1.1. *Let k, l be relatively prime and less than or equal to n. Then*

$$m_n^{k,l}(i, j) = \frac{n!}{kl}.$$

This theorem is striking because the right-hand side of the equality does not depend on i, j. It is easy to prove algebraically based on results of Gordon [4] and Roselle [6]. This was done in a paper of Barcelo, Maule, and Sundaram [1], where they also provided combinatorial proofs of special cases of this result. Here we will give a bijective proof with no restrictions other than those in the statement of the theorem. These restrictions are necessary since the result is no longer true without them. However, we will generalize our bijection to cover the case where the moduli are allowed to have a common factor and prove the following.

Theorem 1.2. *Let k, l be relatively prime and let $d \geqslant 1$. Then*

$$m_n^{kd,ld}(i, j) = \frac{m_n^{d,d}(i, j)}{kl}.$$

The second half of the paper will be devoted to investigating $m_n^{k,l}(i, j)$ when $k = l$. We will give an explicit formula for $m_n^{n,n}(i, j)$. It will also be shown that when $k = l$ is a prime power, the matrix whose (i, j)th entry is $m_n^{k,k}(i, j)$ has a nice block form. Our tools will include restricted shuffles and results from the representation theory of the symmetric group.

Dedication. Bob Maule was an accomplished actuary who took an early retirement due to health problems. After a few years, he enrolled in the graduate program in mathematics at Arizona State University, for the sheer pleasure of doing mathematics.

During a combinatorics course taught by Hélène Barcelo, Bob became quite interested in a question which she was investigating with Sheila Sundaram, namely, the distribution of the values of the major index among the permutations of S_n. He worked relentlessly for several months, analyzing the patterns that were slowly emerging from his computations. This is how he came to develop a matrix approach that we further develop and use here. His contributions to the solution of the original problem were crucial, and led to a joint paper with Hélène and Sheila [1]. Despite serious health problems he continued his computations which foreshadowed several of the results in Section 5. Unfortunately, Bob passed away before he could properly formalize his ideas.

It is undoubtedly his enthusiasm and hard work that brought Hélène back to this subject. She always felt that it was an honor to be his advisor. He was an exceptional person, a constant source of inspiration and a very enjoyable person to work with. He deserves our respect both as a person and as a nascent mathematician.

In tribute to Bob's inspirational work, we are happy to dedicate this article to his memory, hoping that in doing so he will be remembered in our community as a graduate student whose sole motivation was the pleasure of doing mathematics.

2. Preliminaries

Before embarking on a proof of Theorem 1.1, we would like to restate it in a form more amenable to bijective arguments. To do so, we will also need another common combinatorial statistic. The *inversion number* of $\pi \in S_n$ is

$$\operatorname{inv}\pi := \#\{(a_i, a_j):\ i < j \text{ and } a_i > a_j\}.$$

Foata and Schützenberger [2] proved bijectively that the statistics maj and inv are equidistributed over S_n. In fact, their bijection can be used to show that the joint distribution of the pair $(\operatorname{maj}\pi, \operatorname{maj}\pi^{-1})$ is the same as that of $(\operatorname{inv}\pi, \operatorname{maj}\pi^{-1})$. It follows that

$$m_n^{k,l}(i,j) = \#\{\pi \in S_n:\ \operatorname{inv}\pi \equiv i \pmod k \text{ and } \operatorname{maj}\pi^{-1} \equiv j \pmod l\}$$

and this is the combinatorial interpretation for these numbers that we will use for most of the rest of the paper. We will also need the corresponding sets

$$M_n^{k,l}(i,j) = \{\pi \in S_n:\ \operatorname{inv}\pi \equiv i \pmod k \text{ and } \operatorname{maj}\pi^{-1} \equiv j \pmod l\}.$$

It will often be convenient to think of these as the (i,j) entries of matrices $m_n^{k,l}$ and $M_n^{k,l}$, respectively.

To see how this change of viewpoint simplifies things, we will give a bijective proof of a weaker form of Theorem 1.1 where we only consider one of the two statistics. We will also need this result in the proof of the theorem itself. Another combinatorial proof of this result can be found in [1], but ours has the advantage of being simpler and not using induction. Let

$$\begin{aligned} m_n^k(i) &:= \#\{\pi \in S_n:\ \operatorname{maj}\pi \equiv i \pmod k\} \\ &= \#\{\pi \in S_n:\ \operatorname{maj}\pi^{-1} \equiv i \pmod k\} \\ &= \#\{\pi \in S_n:\ \operatorname{inv}\pi \equiv i \pmod k\}. \end{aligned}$$

Proposition 2.1. *If $k \leqslant n$ then*

$$m_n^k(i) = \frac{n!}{k}.$$

Proof. It suffices to show that S_n can be partitioned into subsets of the form $S = \{\pi_0, \dots, \pi_{k-1}\}$ where

$$\operatorname{inv}\pi_i \equiv \operatorname{inv}\pi_0 + i \pmod{k} \tag{1}$$

for $0 \leqslant i < k$. Given $\pi = a_1 a_2 \dots a_n \in S_n$, we construct the subset S containing it as follows. Let a_m be the minimal element of the prefix $a_1 a_2 \dots a_k$ of π. Let σ be the sequence formed from π by removing a_m. Finally, form π_i by inserting a_m into the ith space of σ, where the space completely to the left of σ is counted as space 0. It is easy to see that Eq. (1) holds, so we are done. □

3. Proofs of Theorems 1.1 and 1.2

In order to prove Theorem 1.1 we will need a nice combinatorial interpretation of $\operatorname{maj}\pi^{-1}$ which we will henceforth write as $\operatorname{imaj}\pi$. In fact, it follows immediately from the definitions that

$$\operatorname{imaj}\pi = \sum_{i+1 \text{ left of } i \text{ in } \pi} i$$

and that is how the reader should think of calculating this number.

Given n and l with $n > l$ we will also need a particular bijection $f = f_l$ from S_n to itself defined as follows. The reader may wish to also read the example at the end of the paragraph while they read the definition. If $\tau = a_1 a_2 \dots a_n$ then let $I = \{i_1 < i_2 < \cdots < i_l\}$ be the indices such that $\pi = a_{i_1} a_{i_2} \dots a_{i_l}$ is a permutation of $[l]$. Let σ be the subsequence of π indexed by $[n] - I$, thus τ is a shuffle of π and σ. Consider $J = \{i_1 + 1, i_2 + 1, \dots, i_l + 1\}$ where the sums are taken modulo n. Then define $\tau' = f_l(\tau)$ to be the shuffle of π and σ such that τ' restricted to J and $[n] - J$ are π and σ, respectively. Note that f_l is clearly bijective since one can construct its inverse in exactly the same manner by just subtracting one from each element of I. By way of illustration, suppose that $n = 7$, $l = 4$, and $\tau = 6371452$. So $I = \{2, 4, 5, 7\}$ corresponding to $\pi = 3142$. Also $\sigma = 675$. Thus $J = \{1, 3, 5, 6\}$ and $\tau' = 3617425$.

If τ is a shuffle of π and σ then it will be useful to let $\operatorname{inv}_\tau(\pi, \sigma)$ denote the number of inversion pairs in τ with one element of the pair in π and the other in σ. If $\tau' = f_l(\tau)$, we claim that

$$\operatorname{inv}_{\tau'}(\pi, \sigma) = \begin{cases} \operatorname{inv}_\tau(\pi, \sigma) + l & \text{if } n \notin I, \\ \operatorname{inv}_\tau(\pi, \sigma) - (n - l) & \text{if } n \in I. \end{cases} \tag{2}$$

To see this, note that since every element of π is less than every element of σ, then an inversion is created every time an element of σ precedes an element of π. If $n \notin I$ then there is no wrap-around when passing from τ to τ' and so there is one new inversion created for each of the l elements of π. If $n \in I$ then a position for an element of π is moved from the back of τ to the front, so $n - l$ elements of σ inversions are lost.

We also define $\operatorname{imaj}_\tau(\pi,\sigma)$ as the subsum of $\operatorname{imaj}\tau$ over those pairs $(i, i+1)$ with $i \in \pi$ and $i+1 \in \sigma$ or vice-versa. Note that for the shuffles considered two paragraphs ago,

$$\operatorname{imaj}_\tau(\pi,\sigma) = 0 \text{ or } l. \tag{3}$$

As a step toward proving Theorem 1.1, we prove the following special case.

Lemma 3.1. *Let l be less than and relatively prime to n. Then*

$$m_n^{n,l}(i,j) = \frac{n!}{nl}.$$

Proof. We claim that the map $f = f_l$ restricts to a bijection from $M_n(i,j)$ to $M_n(i+l,j)$. Keeping the notation from the definition of f and using Eq. (2), we see that

$$\begin{aligned}
\operatorname{inv}\tau' &= \operatorname{inv}\pi + \operatorname{inv}\sigma + \operatorname{inv}_{\tau'}(\pi,\sigma) \\
&\equiv \operatorname{inv}\pi + \operatorname{inv}\sigma + \operatorname{inv}_{\tau}(\pi,\sigma) + l \pmod n \\
&\equiv \operatorname{inv}\tau + l \pmod n.
\end{aligned}$$

Thus the row indices in M_n change as desired. For the columns note that, by Eq. (3),

$$\begin{aligned}
\operatorname{imaj}\tau' &= \operatorname{imaj}\pi + \operatorname{imaj}\sigma + \operatorname{imaj}_{\tau'}(\pi,\sigma) \\
&\equiv \operatorname{imaj}\pi + \operatorname{imaj}\sigma \pmod l \\
&\equiv \operatorname{imaj}\tau \pmod l.
\end{aligned}$$

Hence f restricts as claimed.

Since l is relatively prime to n, the set of multiples of l intersects every congruence class modulo n. So iterating f will establish bijections between the sets $M_n(1,j), M_n(2,j), \dots, M_n(n,j)$ for any j. But then by Proposition 2.1 we must have

$$m_n^{n,l}(i,j) = \frac{m_n^l(j)}{n} = \frac{n!}{nl}$$

as desired. □

The previous lemma will form the base case for an inductive proof of Theorem 1.1. For the induction step, we will need a restricted type of shuffle. We let $\pi \sqcup\!\sqcup \sigma$ denote the set of shuffles of the sequences π and σ, e.g.,

$$12 \sqcup\!\sqcup 43 = \{1243,\ 1423,\ 1432,\ 4123,\ 4132,\ 4312\}.$$

We extend this notation (and all future variants of it) to sets by letting $M \sqcup\!\sqcup N = \bigcup(\pi \sqcup\!\sqcup \sigma)$ where the union is over all $\pi \in M$ and $\sigma \in N$.

In order to get a set of permutations from shuffling two permutations, define $\pi \sqcup\!\sqcup^+ \sigma = \pi \sqcup\!\sqcup \tau$ where τ is the sequence formed by adding $|\pi|$ to every element of σ. For example $12 \sqcup\!\sqcup^+ 21$ would give the same set as displayed above.

We will also need to specify where the copy of π (and thus of σ) occurs in a shuffle. So given $M \subseteq S_l$, $N \subseteq S_{n-l}$, and $I = \{i_1, i_2, \ldots, i_l\} \subseteq [n]$, we define $M \bigsqcup_I^+ N$ to be all permutations $\tau = a_1 a_1 \ldots a_n \in M \bigsqcup^+ N$ such that $a_{i_1} a_{i_2} \ldots a_{i_l} \in M$. By way of illustration

$$\{12,\ 21\} \bigsqcup_{\{2,5\}}^+ \{231,\ 321\} = \{41532,\ 42531,\ 51432,\ 52431\}.$$

Note that if $\pi \in M$ and $\sigma \in N$ then $\operatorname{inv}_\tau(\pi, \sigma)$ is constant for all $\tau \in M \bigsqcup_I^+ N$. So define the *weight of* I, $\operatorname{wt} I$, to be this constant value

$$\operatorname{wt} I = \sum_{i \in I} i - \binom{l+1}{2}.$$

The next result will permit us to complete the proof of Theorem 1.1. In it, $\uplus$ denotes disjoint union.

Lemma 3.2. *Given n, k, l with $n \geqslant l$, we have*

$$M_n(i, j) = \biguplus \left[M_l(i', j') \bigsqcup_I^+ M_{n-l}(i'', j'') \right]$$

where the disjoint union is over all i', j', i'', j'', I such that

$$i \equiv i' + i'' + \operatorname{wt} I \pmod{k} \quad \textit{and} \quad j \equiv j' + j'' \pmod{l}.$$

Proof. To show that the right-hand side is contained in the left, let $\tau = \pi \bigsqcup_I^+ \sigma$ where $\pi \in M_l(i', j')$ and $\sigma \in M_{n-l}(i'', j'')$. Then

$$\operatorname{inv} \tau = \operatorname{inv} \pi + \operatorname{inv} \sigma + \operatorname{inv}_\tau(\pi, \sigma) = i' + i'' + \operatorname{wt} I \equiv i \pmod{k}.$$

Also, since $\pi \in S_l$, we have

$$\operatorname{imaj} \tau = \operatorname{imaj} \pi + \operatorname{imaj} \sigma + \operatorname{imaj}_\tau(\pi, \sigma) \equiv j' + j'' \equiv j \pmod{l}.$$

Thus $\tau \in M_n(i, j)$.

To show the reverse containment, suppose $\tau \in M_n(i, j)$ is given. Let I be the indices where the elements of $[l]$ appear in τ. Also let π and σ be τ restricted to I and to $[n] - I$, respectively (where l has been subtracted from every element of the latter restriction). Then $\tau = \pi \bigsqcup_I^+ \sigma$ with $\pi \in M_l(i', j')$ and $\sigma \in M_{n-l}(i'', j'')$ for i', i'', j', j'' satisfying the equations in the statement of the lemma. Hence we are done. □

As an application of the two previous lemmas, let us reprove a result from [1] which we will need later.

Corollary 3.3. *We have*

$$m_{n+1}^{n,n}(i, j) = m_n^{n,n}(i, j) + (n-1)!.$$

Proof. In Lemma 3.2, replace n by $n+1$ and let $k=l=n$. Note that $M_1(i'',j'')=\{1\}$ when $i''=j''=0$ and is the empty set otherwise. So taking cardinalities we obtain

$$m_{n+1}(i,j)=\sum_{i',I} m_n(i',j).$$

Now note that we must have $I=[n+1]-\{a\}$ for some $a\in[n+1]$. It follows that $\operatorname{wt} I = n+1-a$ and thus, modulo n, $\operatorname{wt} I$ takes on the values $1,\dots,n-1$ each exactly once and the value 0 twice. Using this fact and Proposition 2.1 gives

$$\sum_{i',I} m_n(i',j)=m_n(i,j)+\sum_{i'=0}^{n-1} m_n(i',j)=m_n(i,j)+(n-1)!$$

which completes the proof. □

We now have all the tools in place to prove Theorem 1.1 which we restate here for convenience.

Theorem 3.4. *Let k,l be relatively prime and less than or equal to n. Then*

$$m_n^{k,l}(i,j)=\frac{n!}{kl}.$$

Proof. We proceed by induction on n. As noted after the original definition, the matrix $m_n^{k,l}$ is the transpose of $m_n^{l,k}$. So it will suffice to prove the result for either $l<k$ or $l>k$ in both the base case and induction step.

We take as our base case when $l<k=n$. But this has already been taken care of by Lemma 3.1.

For the induction step we assume $k<l<n$. We can appeal to the base case to see that $m_l(i,j)$ is independent of i,j. Thus there are bijections between any two sets of the form $M_l(i,j)$. We will now construct a bijection between $M_n(i,j)$ and $M_n(i,j+1)$. By Proposition 2.1, this will finish the proof. Decompose these two sets as in Lemma 3.2. Then, since i is being held constant, every set $M_{n-l}(i'',j'')$ appearing in the expansion of the $M_n(i,j)$ also occurs in that of $M_n(i,j+1)$. The only difference is that in the first expansion it is shuffled with $M_l(i',j')$ and in the second with $M_l(i',j'+1)$. But there is a bijection between these two sets and so also between the corresponding shuffles. It follows that we have a bijection between the disjoint unions, i.e., between $M_n(i,j)$ and $M_n(i,j+1)$. □

As already mentioned, the previous theorem is not true as stated if k,l are not relatively prime and we shall see some examples of this in the next section dealing with the case when $k=l$. However, one can extend this result to the case where the parameters have a greatest common divisor d, for any $d\geqslant 1$, as follows.

Theorem 3.5. *Let k,l be relatively prime and let $d\geqslant 1$. Then*

$$m_n^{kd,ld}(i,j)=\frac{m_n^{d,d}(i,j)}{kl}.$$

Otherwise put, $m_n^{kd,ld}$ admits a block decomposition into kl submatrices of dimension $d \times d$, each of which equals $\frac{1}{kl} m_n^{d,d}$.

Proof. The proof is similar to that of Theorem 3.4. So we will merely sketch it, adding details only when there are significant differences from the previous proof.

We first need an analogue of Proposition 2.1 which is that

$$m_n^{kd,d}(i,j) = \frac{m_n^{d,d}(i,j)}{k} \tag{4}$$

for any k with $n \geqslant kd$. To show this, it suffices to find a bijection

$$g : M_n^{kd,d}(i,j) \to M_n^{kd,d}(i+d,j)$$

for all i, j since then

$$m_n^{d,d}(i,j) = \sum_{i'} m_n^{kd,d}(i',j) = k m_n^{kd,d}(i,j)$$

where the sum is over all i' with $i' \equiv i \pmod d$ and $1 \leqslant i' \leqslant kd$. Given $\tau \in M_n^{kd,d}(i,j)$, write $\tau = \pi \bigsqcup_I^+ \sigma$ where π is the subsequence of τ which is a permutation of $[kd]$, which also uniquely determines σ and I. Define $g(\tau) = f_d(\pi) \bigsqcup_I^+ \sigma$ where f_d is the map defined at the beginning of this section. It is easy to verify, using computations similar to those in Lemma 3.1, that $g(\tau) \in M_n^{kd,d}(i+d,j)$ and that g is invertible. So this proves Eq. (4).

Next we need a version of Lemma 3.1 itself which is

$$m_{kd}^{kd,ld}(i,j) = \frac{m_{kd}^{d,d}(i,j)}{kl} \tag{5}$$

for k, l relatively prime and $l < k$. Recalling that $m_n^{k,l}$ and $m_n^{l,k}$ are transposes, Eq. (4) can be rewritten

$$m_n^{d,ld}(i,j) = \frac{m_n^{d,d}(i,j)}{l}.$$

We also have

$$m_n^{d,ld}(i,j) = \sum_{i'} m_n^{kd,ld}(i',j)$$

where the sum is over all i' with $i' \equiv i \pmod d$ and $1 \leqslant i' \leqslant kd$. So to prove Eq. (5), it suffices to find a bijection between $M_{kd}^{kd,ld}(i,j)$ and $M_{kd}^{kd,ld}(i+d,j)$ for all i, j. Using f_{ld} gives a bijection between $M_{kd}^{kd,ld}(i,j)$ and $M_{kd}^{kd,ld}(i+ld,j)$. But since k and l are relatively prime, iteration of this map eventually produces the desired bijection and we have Eq. (5).

Finally, we need an induction on n to prove the full result, where the previous paragraph gives us the base case when $n = kd$ (assuming, without loss of generality, that $l < k$). But now Lemma 3.2 can be used in much the same way as in the proof of Theorem 3.4 to complete the induction step. Specifically, this Lemma can be used to lift the bijections in $M_{kd}^{kd,ld}$ to bijections between $M_n^{kd,ld}(i,j)$ and $M_n^{kd,ld}(i,j+d)$ for all i,j. By transposition, we also get bijections between $M_n^{kd,ld}(i,j)$ and $M_n^{kd,ld}(i+d,j)$. Then the proof is finished by noting that

$$m_n^{d,d}(i,j)=\sum_{i',j'} m_n^{kd,ld}(i',j')$$

where the sum is over all i',j' with $i'\equiv i \pmod d$, $j'\equiv j \pmod d$, $1\leqslant i'\leqslant kd$, and $1\leqslant j'\leqslant ld$. □

4. The case $k=l$

Theorem 3.5 reduces computation of the matrices $m_n^{k,l}$ to the case where $k=l$ which we will now consider. We first derive a formula for the special case $m_n^{n,n}(i,j)$. We will use techniques from the representation theory of the symmetric group S_n. More information about these methods can be found in the texts of Sagan [7] or Stanley [9, Chapter 7]. To state our result, we use μ and ϕ for the number-theoretic Möbius and Euler totient functions, respectively. We also let $i\wedge j$ denote the greatest common divisor of i and j.

Theorem 4.1. *Let* $1\leqslant i,j\leqslant n$. *Then*

$$m_n^{n,n}(i,j)=\frac{1}{n^2}\sum_{d|n} d^{n/d}(n/d)!\phi(d)^2\frac{\mu(\frac{d}{i\wedge d})\mu(\frac{d}{j\wedge d})}{\phi(\frac{d}{i\wedge d})\phi(\frac{d}{j\wedge d})}. \tag{6}$$

Proof. Let ω be a primitive nth root of unity and consider the character ω^i of the cyclic subgroup of S_n generated by an n-cycle. Let $\chi_{n,i}$ denote the character obtained by inducing ω^i up to S_n. It is easy to see that $\chi_{n,i}$ is only nonzero on conjugacy classes of type $d^{n/d}$ where $d|n$. On these classes, Foulkes [3] showed that its value is

$$\frac{1}{n}d^{n/d}(n/d)!\phi(d)\frac{\mu(\frac{d}{i\wedge d})}{\phi(\frac{d}{i\wedge d})}.$$

It follows that the inner product $\langle\chi_{n,i},\chi_{n,j}\rangle$ is given by the right-hand side of Eq. (6).

The following fact was discovered independently by Kraśkiewicz and Weyman [5], and by Stanley [9, Exercise 7.88 b]. The multiplicity in $\chi_{n,i}$ of the irreducible character of S_n indexed by a partition λ is the number, $f_{n,i}^{\lambda}$, of standard Young tableaux of shape λ with major index congruent to i modulo n. Using the decomposition into irreducibles we obtain

$$\langle\chi_{n,i},\chi_{n,j}\rangle=\sum_{\lambda\vdash n} f_{n,i}^{\lambda} f_{n,j}^{\lambda}.$$

But via the Robinson–Schensted correspondence one sees that this sum is exactly $m_n^{n,n}(i,j)$, so we are done. □

Using this theorem to calculate the matrices $m_n^{n,n}$ for the values $3\leqslant n\leqslant 5$ gives the following table. (For $n=1,2$ we just get identity matrices.)

$$m_3^{3,3} = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix},$$

$$m_4^{4,4} = \begin{bmatrix} 3 & 1 & 1 & 1 \\ 1 & 2 & 1 & 2 \\ 1 & 1 & 3 & 1 \\ 1 & 2 & 1 & 2 \end{bmatrix},$$

$$m_5^{5,5} = \begin{bmatrix} 8 & 4 & 4 & 4 & 4 \\ 4 & 5 & 5 & 5 & 5 \\ 4 & 5 & 5 & 5 & 5 \\ 4 & 5 & 5 & 5 & 5 \\ 4 & 5 & 5 & 5 & 5 \end{bmatrix}.$$

As an application of this theorem, we note the following useful result.

Corollary 4.2. *Suppose $i \wedge n = i' \wedge n$ and $j \wedge n = j' \wedge n$ where $1 \leqslant i, i', j, j' \leqslant n$. Then*

$$m_n^{n,n}(i, j) = m_n^{n,n}(i', j').$$

So to determine the matrix $m_n^{n,n}$ it suffices to determine the entries $m_n^{n,n}(i, j)$ when i and j divide n. Similarly, the numbers $m_{n+1}^{n,n}(i, j)$ only depend on $i \wedge n$, $j \wedge n$, and n.

Proof. The first part follows immediately from Eq. (6) and the fact that we have

$$i \wedge d = (i \wedge n) \wedge d$$

whenever $d|n$. The second part follows from the first and Corollary 3.3. □

The previous theorem will be useful for the base cases of various inductive proofs. To do the induction step, we will need a type of shuffle $\pi \sqcup\!\sqcup_\gamma^+ \sigma$ where the distances between elements of π are restricted. Suppose $\gamma = (g_1, g_2, \ldots, g_{l-1})$ is a composition (ordered partition) and $l = |\pi|$. Let $\pi \sqcup\!\sqcup_\gamma^+ \sigma$ be the set of all shuffles in $\pi \sqcup\!\sqcup^+ \sigma$ such that if the elements of π are at indices $I = \{i_1 < i_2 < \cdots < i_l\}$ then $i_{t+1} - i_t = g_t$ for $1 \leqslant t < l$. By way of illustration,

$$132 \sqcup\!\sqcup_{(1,2)}^+ 321 = \{136254,\ 613524,\ 651342\}.$$

In this situation, we also define the *weight* of the composition to be

$$\operatorname{wt} \gamma = \operatorname{inv}_\tau(\pi, \sigma) = \sum_{t=1}^{l-1} (g_t - 1)(l - t)$$

where τ is the shuffle in $\pi \sqcup\!\sqcup_\gamma^+ \sigma$ whose first element coincides with the first element of π. In the example above

$$\operatorname{wt}(1, 2) = \operatorname{inv}_{136254}(132, 654) = 1.$$

Lemma 4.3. *Given n, l with $n \geqslant l$, we have*

$$M_n^{l,l}(i,j) = \biguplus \left[M_l^{l,l}(i',j') \bigsqcup\nolimits_\gamma^+ M_{n-l}^{l,l}(i'',j'') \right] \tag{7}$$

where the disjoint union is over all i', j', i'', j'', γ such that

$$i \equiv i' + i'' + \operatorname{wt}\gamma \pmod{l} \quad \textit{and} \quad j \equiv j' + j'' \pmod{l}.$$

Proof. The proof is much the same as that of Lemma 3.2, just noting that since $|\pi| = l$ we have $\operatorname{inv}_\tau(\pi,\sigma) \equiv \operatorname{wt}\gamma \pmod{l}$ for all $\tau \in \pi \bigsqcup_\gamma^+ \sigma$. □

5. Primes and prime powers

We now specialize to the case where n is a prime p. Then the sum in (6) simplifies greatly and we can readily write down the entries of the matrix. To do so conveniently in block form, let $J_{k,l}$ be the $k \times l$ all ones matrix. We can also use Corollary 3.3 to give the entries for the associated matrix from S_{p+1}.

Proposition 5.1. *Let p be prime. Then we have*

$$M_p^{p,p} = \frac{(p-1)!}{p} J_{p,p} + \frac{1}{p} \begin{bmatrix} (p-1)^2 J_{1,1} & -(p-1) J_{1,p-1} \\ -(p-1) J_{p-1,1} & J_{p-1,p-1} \end{bmatrix}$$

and

$$M_{p+1}^{p,p} = M_p^{p,p} + (p-1)! J_{p,p}.$$

In fact, we have the same block decomposition for $M_n^{p,p}$ whenever n is a multiple of p or one more than a multiple of p.

Theorem 5.2. *For each prime p there are nonnegative integer sequences $(q_n)_{n\geqslant 1}$, $(r_n)_{n\geqslant 1}$, and $(s_n)_{n\geqslant 1}$, such that*

$$M_{np}^{p,p} = \begin{bmatrix} q_n J_{1,1} & r_n J_{1,p-1} \\ r_n J_{p-1,1} & s_n J_{p-1,p-1} \end{bmatrix}.$$

The matrices $M_{np+1}^{p,p}$ have the same block decomposition (for three other sequences).

Proof. We will prove the result for S_{np} as the one for S_{np+1} is proved similarly. We proceed by induction on n, with the previous proposition providing the base case.

Since M_{np} is symmetric, the statement in the theorem is equivalent to showing that for any $i \geqslant 0$ and any $1 \leqslant j < p-1$ we have $m_{np}(i,j) = m_{np}(i,j+1)$. Decompose both sides of this equation using Lemma 4.3 with $l = p$ and n replaced by np. Note that by the choice of l and n, induction applies to the matrices on the right-hand side of (7). Furthermore, since i is being held constant, the same i', i'', and γ will occur in the expansions for the (i,j) and $(i,j+1)$ entries. Also, the equation $j \equiv j' + j'' \pmod{p}$ has precisely p solutions of which exactly two involve zero because of the range of j. But the same can be said of $j+1$. Thus when one takes cardinalities in (7), the two summations will have identical summands. Hence we are done. □

When n is a prime power p^r, then the sum (6) also simplifies. Using Corollary 4.2 and symmetry, one sees that to determine the matrix for this value of n we need only compute $m_n^{n,n}(p^i, p^j)$ for $i \leqslant j$. In fact, because of zero terms in the sum, for given i all the values for $j > i$ are equal.

Proposition 5.3. *Suppose $n = p^r$ where p is prime and $0 \leqslant i \leqslant j \leqslant r$. The matrix $m_n^{n,n}$ is completely determined by the values*

$$m_n^{n,n}(p^i, p^j) = \frac{1}{p^{2r}} \sum_{k=0}^{i+1} (p^k)^{p^{r-k}} (p^{r-k})! \phi(p^k)^2 \psi(i, j, k)$$

where

$$\psi(i, j, k) = \begin{cases} 1 & \text{if } k \leqslant i, \\ \dfrac{1}{(p-1)^2} & \text{if } k = i+1 \text{ and } i = j, \\ \dfrac{-1}{p-1} & \text{if } k = i+1 \text{ and } i < j. \end{cases}$$

Similarly, Theorem 5.2 and its proof can be extended without difficulty to the following result.

Theorem 5.4. *Suppose $k = l = p^r$ where p is prime and $0 \leqslant i \leqslant j \leqslant r$. The matrix $m_{np^r}^{p^r, p^r}$ is completely determined by its entries in positions (p^i, p^j). Furthermore, given i all these entries for $j > i$ are equal. The same is true for the matrix $m_{np^r+1}^{p^r, p^r}$.*

In general, it is not easy to explicitly compute the sequences $(q_n)_{n\geqslant 1}$, $(r_n)_{n\geqslant 1}$, and $(s_n)_{n\geqslant 1}$ in Theorem 5.2 because the expression (7) of Lemma 4.3 is so complicated. But when $p = 2$ things simplify greatly and we also get equality of the diagonal elements which is not true in general.

To state our results compactly, let $B_n = M_n^{2,2}$ and similarly for the matrix b_n. Also, if Γ is a set of compositions of length $|\pi| - 1$ then let

$$\pi \bigsqcup\nolimits_\Gamma^+ \sigma = \biguplus_{\gamma\in\Gamma} \left(\pi \bigsqcup\nolimits_\gamma^+ \sigma\right).$$

Finally, let

$$O = \{1, 3, 5, \ldots\} \quad \text{and} \quad E = \{2, 4, 6, \ldots\}.$$

The next theorem follows easily from Lemma 4.3 and induction, so we will merely state it. None of the sequences mentioned in this result have been previously submitted to Sloane's encyclopedia [8].

Theorem 5.5. *Suppose $n \geqslant 2$.*

(1) $B_n(i,j) = \big(12 \sqcup\!\sqcup_O^+ B_{n-2}(i,j)\big) \uplus \big(12 \sqcup\!\sqcup_E^+ B_{n-2}(i+1,j)\big) \uplus$
$\big(21 \sqcup\!\sqcup_E^+ B_{n-2}(i,j+1)\big) \uplus \big(21 \sqcup\!\sqcup_O^+ B_{n-2}(i+1,j+1)\big)$.

(2) $b_{2n}(i,j) = 2n^2 b_{2n-2}(i,j) + 2n(n-1) b_{2n-2}(i+1,j)$,
$b_{2n+1}(i,j) = 2n(n+1) b_{2n-1}(i,j) + 2n^2 b_{2n-1}(i+1,j)$.

(3) *The matrices $c_{2n} := b_{2n}/(2^{n-1}n!)$ and $c_{2n+1} := b_{2n+1}/(2^{n-1}n!)$ have integer entries satisfying*

$$c_{2n}(i,j) = n c_{2n-2}(i,j) + (n-1) c_{2n-2}(i+1,j),$$
$$c_{2n+1}(i,j) = (n+1) c_{2n-1}(i,j) + n c_{2n-1}(i+1,j).$$

(4) $b_n(i,j) = b_n(i+1,j+1)$.
(5) $b_{2n} = (2n) b_{2n-1}$.

References

[1] H. Barcelo, R. Maule, S. Sundaram, On counting permutations by pairs of congruence classes of major index, Electron. J. Combin. 9 (1) (2002). Research Paper 21, 10 pp. (electronic).
[2] D. Foata, M.-P. Schützenberger, Major index and inversion number of permutations, Math. Nachr. 83 (1978) 143–159.
[3] H.O. Foulkes, Characters of symmetric groups induced by characters of cyclic subgroups, in: Combinatorics, Proc. Conf. Combinatorial Math., Math. Inst., Oxford, 1972, Inst. Math. Appl., Southend, 1972, pp. 141–154.
[4] B. Gordon, Two theorems on multipartite partitions, J. London Math. Soc. 38 (1963) 459–464.
[5] W. Kraśkiewicz, J. Weyman, Algebra of coinvariants and the action of a Coxeter element, Bayreuth. Math. Schr. 63 (2001) 265–284.
[6] D.P. Roselle, Coefficients associated with the expansion of certain products, Proc. Amer. Math. Soc. 45 (1974) 144–150.
[7] B.E. Sagan, The Symmetric Group, in: Representations, combinatorial algorithms, and symmetric functions, second ed., in: Grad. Texts in Math., vol. 203, Springer-Verlag, New York, 2001.
[8] N.J.A. Sloane, The on-line encyclopedia of integer sequences, Notices Amer. Math. Soc. 50 (8) (2003) 912–915.
[9] R.P. Stanley, Enumerative combinatorics, vol. 2, Cambridge Stud. Adv. Math., vol. 62, Cambridge University Press, Cambridge, 1999. With a foreword by G.-C. Rota and Appendix 1 by S. Fomin.